Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of reporting malware events comprising the steps of:

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event [[,]] over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time[[.]] so as to prevent network congestion that adversely affects the usability of the network.

2. – 15. (Cancelled)

16. (Previously Presented) The method of claim 1, wherein the method further comprises the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

17. (Currently Amended) A system for reporting malware events comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event [[,]] over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that

could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time[[.]] so as to prevent network congestion that adversely affects the usability of the network.

18. - 31. (Cancelled)

32. (Previously Presented) The system of claim 17, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

33. (Currently Amended) A computer program product for reporting malware events, comprising:

a computer readable storage medium;

computer program instructions, recorded on the computer readable storage medium, executable by a processor, for performing the steps of

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event [[,]] over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time[[.]] so as to prevent network congestion that adversely affects the usability of the network.

34. – 47. (Cancelled)

48. (Previously Presented) The computer program product of claim 33, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

49. (Previously Presented) The method of claim 1, wherein the event trigger threshold is set at a management server in a malware management program.

50. (Previously Presented) The method of claim 49, wherein the event trigger threshold is set by setting policies in the malware management program.

51. (Previously Presented) The method of claim 1, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

52. (Previously Presented) The method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

53. (Previously Presented) The method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

54. (Previously Presented) The method of claim 1, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

55. (Previously Presented) The method of claim 54, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

56. (Previously Presented) The method of claim 54, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

57. (Previously Presented) The method of claim 54, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

58. (Previously Presented) The method of claim 54, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

59. (Previously Presented) The method of claim 54, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

60. (Previously Presented) The system of claim 17, wherein the event trigger threshold is set at a management server in a malware management program.

61. (Previously Presented) The system of claim 60, wherein the event trigger threshold is set by setting policies in the malware management program.

62. (Previously Presented) The system of claim 17, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

63. (Previously Presented) The system of claim 17, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

64. (Previously Presented) The system of claim 17, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

65. (Previously Presented) The system of claim 17, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

66. (Previously Presented) The system of claim 65, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

67. (Previously Presented) The system of claim 65, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

68. (Previously Presented) The system of claim 65, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

69. (Previously Presented) The system of claim 65, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

70. (Previously Presented) The system of claim 65, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

71. (Previously Presented) The computer program product of claim 33, wherein the event trigger threshold is set at a management server in a malware management program.

72. (Previously Presented) The computer program product of claim 71, wherein the event trigger threshold is set by setting policies in the malware management program.

73. (Previously Presented) The computer program product of claim 33, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

74. (Previously Presented) The computer program product of claim 33, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

75. (Previously Presented) The computer program product of claim 33, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

76. (Previously Presented) The computer program product of claim 33, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

77. (Previously Presented) The computer program product of claim 76, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

78. (Previously Presented) The computer program product of claim 76, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

79. (Previously Presented) The computer program product of claim 76, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

80. (Previously Presented) The computer program product of claim 76, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

81. (Previously Presented) The computer program product of claim 76, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.